

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UNITED STATES OF AMERICA)	
)	No. 14 CR 319
v.)	
)	Judge Virginia M. Kendall
KE GU)	

**GOVERNMENT'S POSITION PAPER AS TO SENTENCING FACTORS AND
OBJECTIONS TO THE PRESENTENCE INVESTIGATION REPORT**

The UNITED STATES OF AMERICA, by its attorney, ZACHARY T. FARDON, United States Attorney for the Northern District of Illinois, respectfully submits its sentencing memorandum with respect to defendant KE GU. In this submission, the government addresses why the defendant should receive a sentence of 12 months' imprisonment, which is the statutory maximum sentence, and almost three years below the otherwise advisory guidelines range of 46 to 57 months' imprisonment. The defendant engaged in a scheme, along with codefendant Jun Xu, to defraud Microsoft and unsuspecting customers by offering, selling, and when requested, shipping, copies of counterfeit Microsoft software. The defendant personally engaged in this conduct, specifically burning and shipping counterfeit copies of the software for over a year before law enforcement searched his property and stopped that end of the scheme. All told, during the defendant's involvement in the scheme, he and his codefendant sold approximately \$1.76 million dollars' worth of counterfeit software. This Court should impose a sentence that reflects the nature of the defendant's crime and inform the public that copyright infringement ultimately hurts other consumers through increased prices for legitimate purchases

of software. Thus, the government respectfully requests that the Court impose a sentence of 12 months' imprisonment.

I. PROCEDURAL BACKGROUND

On June 3, 2014, the defendant and codefendant Jun Xu were charged by way of indictment for a mail fraud scheme to sell and ship counterfeit Microsoft software, in violation of Title 18, United States Code, Section 1341, and one count of copyright infringement, in violation of Title 17, United States Code, Section 506(a)(1)(A) and Title 18, United States Code, Section 2319(b)(1). Document #1.

On January 15, 2016, the defendant was charged by way of a superseding information with one count of misdemeanor copyright infringement, in violation of Title 17, United States Code, Section 506(a)(1)(A) and Title 18, United States Code, Section 2319(b)(3). Document #41.

On January 18, 2016, the defendant pled guilty to the superseding information. Document #45. The sentencing hearing is currently scheduled for February 7, 2016, at 1:00 p.m.

II. FACTUAL BACKGROUND

From in or about August 2010, and through in or about October 2011, at Naperville, in the Northern District of Illinois, Eastern Division, and elsewhere, the defendant and others known and unknown, did willfully, for the purpose of private financial gain, infringe the copyrights of copyrighted works, that is, computer software of Microsoft Corporation, by the reproduction and distribution by

electronic and physical means, including by means of the Internet and the United States Postal Service.

More specifically, codefendant Jun Xu owned and operated the websites www.elecsurf.com and www.pcdeal4u.com, and owned and used the email addresses admin@elecsurf.com, orders@pcdeal4u.com, and store@pcdeal4u.com, to conduct transactions and communicate with customers and the defendant.

The websites offered various software products for less than the manufacturer's suggested retail price. Xu accepted credit card payments for the software purchases through the websites and also maintained numerous personal and business bank accounts in his name and in the name of the websites.

Xu operated the websites and advertised numerous copyrighted software products for sale that he was not authorized to sell. Xu offered the copyrighted software products at a significant discount from the MSRP for each product. For each copyrighted software product for sale, Xu falsely advertised that each copyrighted software product was authentic and that the purchaser would be provided with a genuine retail product license key.

Customers who visited the websites were able to select which copyrighted software products to purchase and pay for the copyrighted software products via a credit card through the websites. Customers also could choose how they wished to receive the copyrighted software products—either via direct download or by paying an additional shipping charge for a physical disc to be mailed to them.

Once the purchase was completed through the websites, Xu, using one of the website email addresses, emailed the customer a confirmation of the customer's order. Xu also included in the email fraudulently obtained Microsoft Developer Network product keys for the copyrighted Microsoft software products, which were used to install the infringed software product.

Neither Xu nor the defendant had authorization from Microsoft to sell any of the copyrighted software products that Xu falsely represented on the websites to be authentic and genuine. Additionally, neither Xu nor the defendant was a member of the Microsoft Developer Network or had authority from Microsoft to issue the Microsoft Developer Network product keys to use with the infringed software products.

If the customer chose to have a disc shipped instead of directly downloading the copyrighted software product, Xu informed customers that he would mail the customers a disc via United States Postal Service. The defendant then shipped the copyrighted software product discs from the defendant's Naperville home. The defendant used computers, printers, and disc duplicating towers to copy and ship the discs.

Specifically, after an order for a disc was placed by a customer, Xu informed the defendant of which copyrighted software product the customer ordered and the customer's mailing address, and instructed the defendant to mail the copyrighted software product to the customer. Inside the defendant's Naperville home, the defendant made a copy of the ordered copyrighted software product onto a DVD-R

and printed the proper USPS postage using Xu's Stamps.com account. The defendant then mailed the DVD-R of the infringed software product to the customer through the USPS. The money from the purchases was deposited into Xu's bank accounts. Xu then paid the defendant for the defendant's role in the copying and mailing of the DVD-R of the infringed software products by depositing a portion of the proceeds from the orders into the defendant's bank accounts.

From on or about August 25, 2010, to on or about August 29, 2011, the defendant knowingly infringed the copyrights of Microsoft copyrighted works by copying and distributing approximately 6,962 Microsoft software products.

As detailed in the spreadsheets attached to the Supplemental Government's Version (dated May 16, 2016), the defendant and codefendant's conduct resulted in a conservative loss amount of approximately \$1.76 million for the software sold electronically and shipped via the USPS from both websites, for which he is jointly and severally liable with codefendant Jun Xu.

III. SENTENCING GUIDELINES RANGE

The government agrees with the advisory guidelines calculation set forth in the Presentence Investigation Report ("PSR"), which concludes that because the statutory maximum sentence of 12 months' is less than the minimum of the advisory guidelines range, the guidelines range equals 12 months' imprisonment. PSR at ¶ 87. However, the government disagrees with the loss attributable to defendant based on his conduct, and that of his codefendant that was reasonably foreseeable to him, during his participation of the scheme.

This Court is “only required to make ‘a reasonable estimate of the loss.’” *United States v. Sullivan*, 765 F.3d 712, 716 (7th Cir. 2014) (citing U.S.S.G. § 2B1.1 cmt. app. n. 3(A)); *United States v. Powell*, 576 F.3d 482, 497 (7th Cir. 2009); *United States v. Watts*, 535 F.3d 650, 658 (7th Cir. 2008). Furthermore, and most importantly, the loss amount is to be determined by the judge at sentencing based on a preponderance of the evidence. *See United States v. Littrice*, 666 F.3d 1053, 1060 (7th Cir. 2012); *United States v. Danford*, 435 F.3d 682, 689 (7th Cir. 2006). A “court [can] determine reasonable foreseeability based on whether [the defendant] demonstrated a substantial degree of commitment to the conspiracy’s objectives, either through his words or his conduct.” *United States v. Sykes*, 774 F.3d 1145, 1151 (7th Cir. 2014), quoting *United States v. Wang*, 707 F.3d 911, 916 (7th Cir. 2013)

Here, the government took a conservative calculation of the loss attributable, and reasonably foreseeable, to defendant. The methodology used is outlined in the first worksheet of the spreadsheet attached to the Supplemental Government’s Version. The starting point was identifying only the transactions from both websites between August 25, 2010, and October 26, 2011, which encompassed the defendant’s personal involvement of burning and shipping actual discs. Next, any shipping amount was deducted from the loss amount. Any charges over \$500 were omitted from the calculation because the websites sold hardware and other non-software items, despite transactions in excess of \$500 could have been for multiple copies or multiple software packages. Also, any transaction that could not be

identified to match a software package for sale on either website was also omitted. The retail price for each infringed product was taken from Microsoft's website in December 2015, which was the most reliable data point for Microsoft's suggested retail price of each piece of software. These prices are also a benefit to the defendant because the software packages available during the timeframe of the scheme were priced lower in 2015 than they were in 2010 and 2011 due to newer versions that were available and a reduction in price of older versions of Microsoft software. This conservative method of calculating the loss amount still resulted in over 27,000 pieces of software sold, approximately 7,000 of which the defendant himself shipped out of his home through the mail.

The entirety of the 27,000 transactions are reasonably foreseeable to defendant for purposes of the loss amount because defendant knew how the scheme operated and he knew he was only shipping discs for those customers who wished a "backup copy" of the software they purchased from either website. The defendant was not in the dark about how the operation ran, nor was he clueless as to what he was doing. His argument that he only be held accountable for only the items he shipped at an estimated loss of \$626,000 should be rejected. The government has taken an extremely conservative approach, consistent with the law in this Circuit, to hold the defendant accountable, by a preponderance of the evidence, for the loss reasonably foreseeable to him based on his admitted conduct in the scheme.

The Court should also reject defendant's contention that it hold him only accountable for \$35,000, because that was the defendant's gain. Defendant's citation

of *United States v. Pu*, 814 F.3d 818, 825 (7th Cir. 2016), is inapposite. *Pu* involved a trade secret case and the dispute about loss was that it was impracticable to determine or adequately measure the harm or cost to the victim to replace the property. *Id.* at 824-825. This is not a trade secret case regarding statistical models of investment instruments and market activity, but the copying of identifiable software packages that were sold for retail purchase.

Accordingly, the government requests that the Court find that the loss amount equals \$1.76 million and a corresponding 16-level enhancement to the base offense level.

Additionally, the government disagrees that the defendant should receive a reduction in the offense level for a minor role. PSR at ¶ 31. The defendant was a partner with the codefendant and gave the websites the ability to ship discs from the United States. The defendant was shipping over 100 pieces of software per week out of his home in Naperville, Illinois. Even taking the PSR's \$89.99 average price per software item and multiplying it by approximately 7,000 items equals \$630,000—a significant sum. The defendant also actively communicated with his codefendant about the operation of the websites and his compensation and sought to be a full partner in the business. This is not the conduct of someone in a minor role. Therefore, the reduction should not apply.

The government therefore argues that the adjusted offense level equal 26 and assuming the defendant receives acceptance of responsibility, a three-level reduction results in an adjusted offense level of 23. The government agrees that the

defendant has a criminal history category of I. However, pursuant to Guideline § 5G1.1, the advisory guidelines range would therefore equal 12 months' imprisonment.

IV. ARGUMENT

A. Analysis of Section 3553(a) Factors

For the reasons stated below, the government asks the Court to sentence the defendant to 12 months' imprisonment.

1. Nature and Circumstances of the Offense, History and Characteristics of the Defendant, and Providing Just Punishment for the Offense

As the facts above demonstrate, defendant engaged in a scheme for almost 14 months with his codefendant to sell counterfeit Microsoft software to unsuspecting customers. The two websites held themselves out to be authorized Microsoft resellers of genuine Microsoft products and included the logos in support of those false claims. But the defendants were not offering the counterfeit products for sale at too steep of a discount that would make it obvious that the software was counterfeit. Rather, it was slightly discounted, but just enough to entice customers to purchase the software from Elecsurf.com and PCDeal4u.com. It was not until customers tried to enter the fraudulently obtained Microsoft Developer Network product keys that some customers realized a scam was afoot. Some of the keys did not work, and when those customers emailed the contact emails of the respective websites, the customers were given additional keys until one worked. However,

many of the product keys did work and customers were using counterfeit software held out to be genuine.

Selling counterfeit software not only hurts the owner of the copyrighted software in lost sales, it also hurts the consumer when copyright owners have to raise the price for subsequent customers. Counterfeit software also can carry malicious spyware and malware and lead to further economic loss and breaches of privacy. In 2013, the International Data Corporation, a market research firm, published a white paper titled “The Dangerous World of Counterfeit and Pirated Software.” The white paper, albeit sponsored by Microsoft, made the following findings, among others: (1) 33 percent of all computer software in the world is counterfeit; (2) 78 percent of downloaded software can expose users to spyware; (3) 36 percent of downloaded counterfeit software includes malicious adware or Trojans; and (4) 20 percent of counterfeit CDs or DVDs infected the user’s computer with Trojans and other malware. See International Data Corporation, The Dangerous World of Counterfeit and Pirated Software (March 2013), <https://news.microsoft.com/download/presskits/antipiracy/docs/IDC030513.pdf>.

Furthermore, the IDC estimated that the direct costs to businesses having to deal with malware from counterfeit software was expected to be \$114 billion. *Id.* Lastly, the potential losses attributable to data breaches because of the counterfeit software were estimated at \$350 billion. *Id.* These losses to both consumers and business are real and those who counterfeit software must be held accountable for their actions.

A sentence of 12 months' imprisonment is also justified by the defendant's history and characteristics and will provide just punishment for the offense. The defendant was a software developer by training and vocation. PSR at ¶¶ 69-76. He has a bachelor's degree in applied physics and a master's degree in business administration. PSR at ¶ 68. The defendant was not an unwitting participant in this scheme. He developed software for a living. He knew about counterfeit software and he knew what he was doing was illegal. If anyone should have known better than to engage in this crime, there would be no better person than him.

Furthermore, during this scheme, the defendant was grossing over \$10,000 per month, or over \$120,000 per year, working as a software developer. PSR at ¶¶ 73-74. In all likelihood, the defendant did not need the \$2,000 to \$3,000 per month he was benefiting from his codefendant by engaging in this scheme. He was not destitute, or struggling to pay his bills, and he even has a healthy 401k. PSR at ¶ 78. By all indications, the defendant engaged in this conduct simply for more money and with the hopes to become a partner with the codefendant to share in the pure profit from the scheme.

The defendant also appears to be a good family man and provider for his wife and children. And as much as that may be a mitigating factor in his favor, he put a seemingly good life and the livelihood of his family at risk by engaging in this crime. Despite the defendant's request for probation, the government argues that based on these 3553(a) factors, in conjunction with others discussed below, such a sentence is not appropriate.

2. *The Need to Promote Respect for the Law and Afford Adequate Deterrence to Criminal Conduct*

The need to promote respect for the law and afford adequate deterrence to criminal conduct also support a sentence of 12 months' imprisonment. The defendant's case presents the Court with an opportunity to impose a sentence that sends both the defendant, his codefendant, and other individuals who profit from selling counterfeit software a clear message that such crimes will not be tolerated. This is the defendant's first contact with the criminal justice system, yet fortunately for the defendant it is a misdemeanor conviction and not a felony. However, his criminal conduct is no less serious than the felony he was originally charged with. The defendant must learn now that committing this type of crime, by a person who is a software developer no less, to unlawfully profit from counterfeit software, is not acceptable and results in real consequences to Microsoft, to customers, to his family, and to himself. A sentence that is too lenient could do little more than cause the defendant to view this conviction and the corresponding sentence as the acceptable cost of being caught.

The imposition 12 months' imprisonment can also further notions of general deterrence. There are segments of the population that view counterfeit software as a victimless crime. However, as explained above, that is far from the truth. And the defendant is not the purchaser, or even a person who does not wish to pay full price for software. Rather, he was on the distribution and seller side of the transactions and his actions furthered the harm to the industry, to Microsoft, and also those who bought counterfeit software to save a few dollars.

This Court should sentence the defendant to 12 months' imprisonment, thereby informing those, either currently engaging in counterfeit software sales, or those thinking about it, to think twice and walk away from such criminal activity.

V. SUPERVISED RELEASE CONDITIONS

As indicated in the PSR, the government agrees with the Probation Officer that the Court impose the following conditions of supervised release:

A. Mandatory Conditions

The government agrees that mandatory conditions 1, 3, 6, and 7 be imposed. PSR at ¶ 93.

B. Discretionary Conditions

The defendant should provide financial support for his dependents, continue to work, and make restitution payments as ordered by the Court in order to support the defendant's rehabilitation and facilitate his satisfaction of his financial obligations and restitution that the Court orders. PSR at ¶ 94(1), (2), (4); 18 U.S.C. § 3663A.

The defendant should refrain from communicating with anyone engaged in criminal activity and also refrain from doing so with the codefendant, Jun Xu, in order to support the defendant's rehabilitation and ensure that he is engaged in lawful pursuits. PSR at ¶ 94(6).

The defendant should not possess a firearm or destructive device, or other dangerous weapon in order to promote deterrence and to protect the public. PSR at ¶ 94(8).

The defendant should: remain in the jurisdiction where he will be supervised; report to the officer as directed; permit the officer to visit him; allow the officer to confiscate contraband; notify the officer of a change in residence or employer, or if arrested or questioned by law enforcement, all in order to facilitate his supervision by the probation officer. PSR at ¶ 94(14)-(18).

C. Special Conditions

The defendant shall perform community service if unemployed at the direction of the Probation Office until gainfully employed, in order to ensure the defendant is engaged in lawful activity. PSR at ¶ 95(3).

The defendant should not incur new lines of credit, provide access to requested financial information, and notify the court of any material change in economic circumstances, and pay any financial penalty as ordered by the Court, in order to facilitate the defendant's satisfaction of financial penalties and restitution. PSR at ¶ 95(5)-(7), (10).

The defendant should not enter into any agreement to act as an informer of law enforcement without permission of the Court and agrees to permit the probation officer to notify third parties of the risk of future crimes, in order to specifically deter the defendant from criminal activity and to protect the public. PSR at ¶ 95(11), (13).

VI. RESTITUTION

Pursuant to 18 U.S.C. § 3663A, defendant is required to pay restitution, jointly and severally with his codefendant, in the amount the Court determines. The

government argues that the amount equals \$1,762,856.47 payable to Microsoft. The Government requests that restitution be made due immediately, to be paid pursuant to a schedule set by the Court at sentencing.

VII. CONCLUSION

In light of the foregoing, the government respectfully requests that this Court impose a sentence of 12 months' imprisonment.

Respectfully submitted,
ZACHARY T. FARDON
United States Attorney

By: s/ Peter S. Salib
PETER S. SALIB
Assistant United States Attorney
219 S. Dearborn Street, 5th Floor
Chicago, Illinois 60604
(312) 697-4092

Dated: February 1, 2016